ПП № 3(46)-2014. стр. 176—180

УДК 343.140.02 + 002: 004 : 343.140.02

Д. В. Овсянников

ЭЛЕКТРОННОЕ КОПИРОВАНИЕ ИНФОРМАЦИИ — ПРОБЛЕМЫ ПРАКТИКИ И НОРМАТИВНОЙ РЕГЛАМЕНТАЦИИ В УПК РФ

D. V. Ovsiannicov

ELECTRONIC INFORMATION DUPLEXING — PROBLEMS OF PRACTICE AND NORMATIVE REGULATION IN THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

В статье исследуются проблемы использования электронного копирования информации в доказывании по уголовным делам. Обосновывается вывод о том, что электронное копирование информации может применяться в ходе обыска, выемки или осмотра, а также заслуживает признания в качестве самостоятельного следственного действия. Однако для этого требуется законодательное закрепление порядка проведения данного познавательного приема. Одной из причин относительно низкой результативности деятельности правоохранительных органов по раскрытию и расследованию компьютерных преступлений видится недостаточная подготовленность следователей и дознавателей к работе с доказательственной информацией, содержащейся на электронных носителях. Действующее уголовно-процессуальное законодательство испытывает значительное отставание от развития современных телекоммуникационных отношений. Это в полной мере относится и к электронному копированию информации.

Ключевые слова: *информация, уголовный процесс, электронное копирование.*

This paper investigates the problem of the use of electronic information duplexing in evidence of criminal cases. The author justifies the conclusion that the electronic information duplexing can be used during the search, seizure or inspection, as well as can be recognized as an independent investigative action. However, this requires legislative consolidation of the procedures of the abovementioned approach. One of the reasons for the relatively poor performance of law enforcement activities in detection and investigation of computer crimes is the insufficient qualification of inquiry officers and investigators to work with evidentiary information which is on electronic media. Current criminal and procedural law is experiencing a significant lag from the development of modern telecommunication relations. This is fully applied to the electronic information duplexing.

Keywords: *information, criminal proceedings, electronic duplexing.*

Стремительное развитие глобальной компьютерной сети Интернет привело к тому, что информационно-телекоммуникационные инфраструктуры промышленно развитых стран, их национальные информационные ресурсы оказались весьма уязвимыми объектами посягательств со стороны террористических организаций, преступных сообществ и групп, а также отдельных криминальных элементов. Массовыми и наиболее прибыльными видами преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий, являются мошенничества и кражи денежных средств со счетов физических лиц и организаций. Так, в 2012 году подразделениями «К» МВД России на всей территории страны зарегистрировано 3645 подобных преступлений, тогда как в 2011 году их было 2123 [3].

Компьютерные системы становятся частью самых разнообразных сфер жизнедеятельности общества, а потому ис-

пользование современных технологий с противоправными целями уже давно вышло за рамки составов компьютерных преступлений. Так, они используются для проектирования и изготовления фальсифицированных документов, денежных знаков, печатей, для создания и хранения баз данных при мошенничестве, лжепредпринимательстве и иных видах преступных деяний. Особому криминальному влиянию подвергнута финансово-кредитная система. Применение современных компьютерных технологий получает все большее распространение в качестве средств совершения и сокрытия различных видов преступлений.

Одновременно защита прав и законных интересов лиц и организаций, потерпевших от преступления становится приоритетным назначением уголовного судопроизводства (ст. 6 УПК РФ). В случае обнаружения признаков преступления прокурор, следователь, орган дознания и дознаватель принимают предусмотренные законом меры по установлению события преступления, изобличению лица или лиц, виновных в совершении преступления (ч. 2 ст. 21 УПК РФ). Уголовно-процессуальные возможности предопределяют реализацию принципа неотвратимости уголовного наказания и во многом на сегодня зависят от успешного использования электронных информационных ресурсов.

Электронное копирование информации как познавательный прием используется в доказывании по уголовным делам. На сегодня оно проводится в рамках обыска, выемки или осмотра. Анализ следственной и судебной практики показывает, что во многих случаях электронное копирование информации может быть востребовано как самостоятельное средство уголовно-процессуального доказывания. Имеются в виду такие ситуации, когда следователя, дознавателя или суд интересует только электронная информация и нет необходимости проводить полномасштабный обыск, выемку или осмотр, будь то жилище, помещение или физическое лицо. При этом проверка допустимости использования доказательств по результатам электронного копирования требует особого внимания.

Так, 4 декабря 2008 года в вечернее время гр. В. и П. группой лиц совершили убийство гр. С. При этом гр. Д. оказал им в этом пособничество. Челябинский областной суд вынес обвинительный приговор. Помимо других доказательств в материалах уголовного дела имеется протокол осмотра предметов от 30 декабря 2008 года, согласно которому наряду с другими предметами был осмотрен сотовый телефон Самсунг SGH-D 840. В ходе просмотра и прослушивания содержащихся на данном телефоне файлов обнаружен файл SM-007. Данный файл содержит в себе фрагмент совершаемого в отношении С. преступления. Этот файл, согласно записи в протоколе, был изъят из осматриваемого телефона путем копирования на память жесткого диска персонального служебного компьютера. Из текста протокола следует, что осмотр предметов производился в присутствии понятых, протокол удостоверен их подписями. Сведений о том, что во время осмотра предметов воспроизводился скопированный с телефона файл SM-007, в протоколе не имеется. Вместе с тем, к протоколу приобщена распечатка, согласно которой во время осмотра предметов на персональном компьютере следователем с помощью программы «ACDSee 8» был воспроизведен скопированный с телефона файл SM-007. Установлено, что данный файл представляет собой цифровую аудиозапись, на которой слышны мужские голоса. Приведено содержание аудиозаписи. Однако данное приложение не заверено подписями понятых, в связи с чем у суда возникли сомнения по поводу их участия при воспроизводстве вышеуказанной аудиозаписи. Кроме того, граждан с указанными фамилиями, значащихся в качестве понятых, в г. Челябинске установить не представилось возможным. В связи с чем, на основании п. 3 ч. 2 ст. 75 УПК РФ суд признал распечатку к протоколу осмотра предметов от 30 декабря 2008 года недопустимым доказательством [10].

Предложения об обособлении электронного копирования информации в качестве самостоятельного следственного действия поступали и ранее [2]. Такое заявление отдельные авторы основывали на различиях в фактической природе обыска, выемки, осмотра, с одной стороны, и электронного копирования информации — с другой. В. А. Семенцов, поддерживая эту идею в целом, пишет: «...в практике расследования возникает необходимость электронного копирования информации, и этот новый познавательный прием соответствует требованиям закона, морали и социальным закономерностям общественного развития. Необходимо только включить электронное копирование в систему процессуальных действий, предназначенных для собирания доказательств» [9, с. 36].

Действительно, развитие компьютерной и иной электронной техники, а также ее широкое внедрение в различные сферы человеческой деятельности вызвало рост числа противоправных действий, объектом и орудием совершения которых являются электронные носители информации. Прежде всего, это относится к компьютерной технике, однако спектр электронных носителей информации на сегодня гораздо шире.

Расследование таких преступлений имеет свою специфику. В обязательном порядке проводятся осмотры мест происшествия и обыски, направленные на обнаружение и изъятие следов преступления. Существует два способа получения такой информации: 1) изъятие всех обнаруженных средств компьютерной и иной техники с последующим изучением имеющейся на ней информации; 2) изучение всей информации на электронных носителях непосредственно во время проведения осмотра или обыска. Последний вариант предполагает последующее копирование информации, которая представляет интерес для уголовного дела, и (или) изъятие магнитных носителей только с такой информацией.

Изъятие всех средств компьютерной техники ускоряет сам процесс расследования, дает возможность направить все силы на поиск иных материальных следов, имеющих отношение к преступлению (документы, технические средства и т. д.); снижает психологическую нагрузку на граждан; не требует привлечения высококвалифицированного специалиста в области компьютерных технологий к непосредственному участию в обыске, так как грамотное изъятие средств компьютерной техники вполне доступно и специалисту средней руки. К несомненным достоинствам такого подхода можно отнести и возможность в последующем более детально, привлекая необходимых специалистов, изучить всю информацию, имеющуюся в памяти компьютера. Это практически исключает возможность пропустить даже профессионально скрытую информацию. Однако, с другой стороны, в ряде случаев существуют чисто технические сложности изъятия всех средств компьютерной техники (объединение в разнообразные сети, возможность потери информации при отключении и т. п.) или такое изъятие просто нецелесообразно. Также следует помнить, что выход из строя компьютерных систем банков и ряда предприятий может привести к полной дезорганизации их работы и значительным материальным убыткам, что грозит претензиями пострадавших организаций. Поэтому иногда рекомендуется применять второй способ: изъятие информации со средств компьютерной техники непосредственно в ходе проведения осмотра или обыска [4, с. 18]. И здесь не обойтись без электронного копирования информации с использованием переносного компьютера, накопителя USB-флеш и т. п.

Возникает вопрос, правомерно ли считать электронное копирование информации составной частью осмотра, обыска и выемки. Некоторые авторы считают, что можно выделить новый вид обыска — обыск средств компьютерной техники [5, с. 12]. Однако представляется, что для ответа на поставленный вопрос необходимо рассматривать не своеобразие тактики проводимых действий или применяемых технических средств, а природу копирования информации, находящейся в компьютере, и сравнивать ее со спецификой указанных следственных действий. Копирование — это процесс получения копий. Электронное копирование осуществляется с использованием магнитных лент, а также гибких и жестких дисков. Независимо от типа и емкости они используют один и тот же принцип долговременного хранения информации в виде намагниченных участков поверхности накопителя. При движении мимо них считывающего устройства в нем возбуждаются импульсы тока. Данные всегда записываются на магнитной поверхности в виде концентрических окружностей, называемых дорожками. Каждая дорожка в свою очередь состоит из нескольких секторов. Количество информации зависит от числа дорожек (называемого плотностью) и общего размера секторов на одной дорожке. Плотность может существенно меняться от диска к диску. Высокая плотность достигается за счет особых свойств магнитного покрытия [7, с. 98, 102].

Таким образом, электронное копирование информации представляет собой процесс создания намагниченных участков поверхности накопителя за счет использования электромагнитного поля. Здесь нет момента передачи физических объектов, что так характерно для производства обыска или выемки (ст. 182—184 УПК РФ). Кроме того, процессу копирования информации, как правило, предшествует активный поиск информации, находящейся в базе данных персонального компьютера, что также вряд ли соответствует специфике осмотра.

Осмотр местности, жилища, предметов и документов производится в це-

лях обнаружения следов преступления (ст. 176 УПК РФ). Такой осмотр предполагает собой поверхностный обзор указанных объектов и исключает активные внутрипоисковые мероприятия. Кроме того, согласно ч. 1 ст. 177 УПК РФ, осмотр места происшествия предполагает лишь изъятие предметов, что, как было нами отмечено, не соответствует характеру производимых действий при электронном копировании информации. При осмотре же предметов законом не предусмотрено ни изъятие, ни копирование, ни производство других каких-либо подобных действий.

Кроме того, в настоящее время электронное копирование информации в организациях и учреждениях может повлечь за собой раскрытие тайны личной переписки и другой информации, касающейся частной жизни граждан. В такой ситуации потребуется судебное решение, тогда как обыск и выемка в помещении того не требует. Возникшее противоречие может привести к нарушению прав граждан, неуважению их чести и достоинства.

К обыску, выемке и осмотру наиболее близок такой познавательный прием, как изъятие электронных носителей информации, который наряду с копированием информации предусмотрен уголовно-процессуальным законом. Изъятие и копирование электронной информации — два относительно автономных познавательных приема, которые при определенных условиях могут быть последовательными и конкурентными относительно друг друга. Изъятие электронных носителей информации вряд ли может претендовать на самостоятельное следственное действие, так как по природе своей схоже с обыском и выемкой.

Однако на практике в некоторых случаях встречаются некорректные формулировки, например, *изъятие видеозаписи с видеорегистратора автомобиля* [11]. В данном случае должно было иметь место или копирование видеозаписи или изъятие видеорегистратора. В литературе также можно встретить предложение о введении в УПК РФ нормы, регламентирующей выемку компьютерной информации из компьютерной сети [8, с. 99], что также выглядит, по нашему мнению, как минимум некорректно. Информацию нельзя изъять, ее можно скопировать, а изъятию подлежит носитель информации.

Исходя из вышеизложенного, можно констатировать, что электронное копирование информации в силу специфики природы этого явления следует рассматривать как самостоятельное следственное действие, которое необходимо закрепить в УПК РФ.

Предложение о придании самостоятельного следственного значения электронного копирования информации не является единственным в этом роде. Многие исследователи сетуют по поводу отсутствия уголовно-процессуальной регламентации возможности, порядка и особенностей использования таких средств [1, с. 224; 6, с. 18—20].

Таким образом, электронное копирование информации может рассматриваться как познавательный прием, выполняемый в рамках проведения обыска, выемки или осмотра, а также заслуживает признания в качестве самостоятельного следственного действия и как элемент нового следственного действия Для реализации этой идеи необходимы детальная проработка вопроса и внесение дополнений в действующий уголовно-процессуальный закон.

References

1. Volevodz A.G. Protivodeistvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva [Counteraction to Computer Crimes: Legal Fundamentals of International Cooperation]. Moscow. Yurlitinform Publ., 2002. 496 p.
2. Zuev S.V., Sutyagin K.I. Elektronnoe kopirovanie informatsii kak samostoyatel'noe sledstvennoe deistvie [Electronic Information Duplexing as a Separate Investigation Activity]. *Sledovatel'*, 2003, No. 4, p. 14-15.
3. Innovatsionnye resheniya dlya bezopasnosti Rossii [Innovative Solutions for the Safety of Russia]. URL: http://mvd.ru/news/item/830615/.
4. Isaeva L. Obysk: rol' spetsialista [Investigative Search: Role of a Specialist]. *Zakonnost'*, 2001, No. 6, p. 17-21.
5. Komissarov V., Gavrilov M., Ivanov A. Obysk s izvlecheniem komp'yuternoi informatsii [Investigative Search with Computor Information Extraction]. *Zakonnost'*, 1999, No. 3, p. 12-15.
6. Krasnova L.B. Komp'yuternye ob"ekty v ugolovnom protsesse i kriminalistike. Kand. dis. (Yuridicheskie nauki) [Computer Objects in Criminal Proceedings and Criminal Science. Thesis of Cand. Sc. Law]. Voronezh, 2005. 202 p.
7. Norton P. Personal'nyi komp'yuter firmy IBM i operatsionnaya sistema MS-DOS [IBM Personal Computer and Operational System MS-DOS]. Moscow. *Radio i svyaz'*, 1991. 416 p.

8. Rossinskaya E.R., Usov A.I. Sudebnaya komp'yuterno-tekhnicheskaya ekspertiza [Judicial Computer and Technical Expertise]. Moscow. Pravo i zakon Publ., 2001. 416 p.
9. Sementsov V.A. Sledstvennye deistviya v dosudebnom proizvodstve (obshchie polozheniya teorii i praktiki) [Investigation Activities in Pre-Trial Proceedings]. Ekaterinburg. 2006. 298 p.
10. Criminal Case No. 2-25/2010. *Arkhiv Chelyabinskogo oblastnogo suda*.
11. Criminal Case No. 10-368/2014. *Arkhiv Chelyabinskogo oblastnogo suda*.

ОВСЯННИКОВ Дмитрий Васильевич, соискатель кафедры уголовно-правовых дисциплин факультета ПСПО, Южно-Уральский государственный университет. 454021. г. Челябинск, пр. Ленина,76. E-mail: dvo-chel@mail.ru

OVSYANNIKOV Dmitry Vasilievich, external PhD student of the Department of Criminal and Legal Disciplines of the Faculty of Law Enforcement Training of South Ural State University. 76, Lenin Av., 454021, Chelyabinsk. E-mail: dvo-chel@mail.ru

For citation: **D. V. Ovsiannicov**. Electronic Information Duplexing — Problems of Practice and Normative Regulation in the Criminal Code of the Russian Federation
Problemy prava (Issues of Law) founders journal № 3 (46). 2014. pp. 176—180.